



**THE JOINT STAFF
WASHINGTON, DC**

Reply ZIP Code:
20318-6000

JUL 16 2002

**MEMORANDUM FOR DEPUTY CHIEF OF NAVAL OPERATIONS (WARFARE
REQUIREMENTS AND PROGRAMS)**

Subject: DISN DAA DECISION ON DON REQUEST TO CONNECT NMCI TO SIPRNET

1. The Defense Information System Network (DISN) Designated Approving Authorities (DAA) met 12 July 2002. The issue was to decide if Department of Navy (DoN) could connect to SIPRNET given that a 22 May 02 CNO letter¹ identified intention to use an unclassified commercial Internet Protocol (IP), Wide Area Network (WAN) to transport classified operational traffic.

2. Current policy identifies the four Designated Approving Authorities (DAA) (NSA, DIA, Joint Staff and DISA) as responsible for the security of the DISN networks (to include SIPRNET)² and those automated information systems that connect to those networks³. An OSD/C3I Memo dated 5 May 97 (attached) mandates Service and Agency use of DISN for Wide Area Network services. Mandated DISN use was again reiterated in both a 17 Aug 00, Navy and DISA Memorandum of Agreement and by a 15 Sept 00 OSD/C3I memo. DISN services are provided through a Global Information Grid (GIG) architecture that uses three separate transport networks: NIPRNET for unclassified information; SIPRNET for SECRET information; and special networks for Top Secret and above information. Any connections and movement of information between these networks are controlled through accredited guarding solutions. The secret and top secret and above networks do not share IP switching infrastructure with the unclassified network or the Internet.

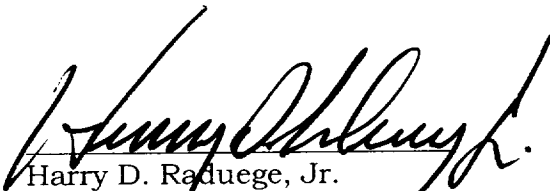
3. Both policy and security aspects of this issue were examined. From a policy perspective, the Navy proposal would significantly change the way DOD transports its operational classified information by using a single, unclassified commercial WAN service as part of its system modernization. While this proposal portends potential future possibilities for DOD systems, it does not follow current policy and proposes a WAN alternative that is inconsistent with the current accepted GIG architecture. The Navy solution allows encrypted classified information to traverse an unclassified network.


4. From a security risk perspective, we reviewed the connection of NMCI to SIPRNET for an increased security risk to SIPRNET and to classified information; and for an increased risk to assuring delivery of classified operational traffic caused by the use of a commercial IP WAN. The conclusions reached were that:


- ♦ The NMCI data protection solution does not increase the security risk to SIPRNET, and adequately protects classified information. It uses NSA certified encryption end-to-end across the IP WAN, and Navy is correcting the vulnerabilities found during NSA's security assessment.
- ♦ NMCI increases operational assurance risk to command and control traffic with the use of an IP WAN that has exposure to non-DOD users, traffic, and commercial switching infrastructure.
- ♦ The proposed use of a commercial WAN presents an unknown security risk in comparison with DISN SIPRNET. Delivery of classified operational traffic could be disrupted through denial of service.


5. NMCI is granted 180 days interim authority to operate (IATO) given the following conditions are met prior to NMCI connection to the SIPRNET:

- DoN provides a letter of accreditation for the NMCI
- DoN uses DISA classified DISN (i.e. SIPRNET) as a service provider
- Where DISA concurs that classified DISN service is unavailable, then DoN is authorized to use the DOD unclassified enclave (NIPRNET Community Of Interest Network Services (COINS)) for that transport leg until such time that DISA confirms availability of SIPRNET services.


 Harry D. Raduege, Jr.
 Lieutenant General, USAF
 Director, Defense Information
 Systems Agency


 Thomas R. Wilson
 Vice Admiral, USN
 Director, Defense Intelligence Agency


 Michael V. Hayden
 Lieutenant General, USAF
 Director, National Security Agency


 Joseph K. Kellogg, Jr.
 Lieutenant General, USA
 Director for Command, Control,
 Communications, and Computer
 Systems Directorate

Enclosure

ASD/C3I memorandum, 5 May 97, "Policy Clarification Letter – Long-Haul and Regional Telecommunications Systems and Services for the Department of Defense (DOD)"

References:

- 1 Chief of Naval Operations letter, 22 May 2002, 5239 Ser N614/2U555077, "Request for Interim Authority To Connect (IATC) NMCI – Secret (NMCI-S) Network Operations Centers (NOC) in Norfolk (CCSC 73SG) and San Diego (CCSD 73SE) Using VBNS+ and COINS for Transport Services"
- 2 CJCSI 6211.02A, 22 May 1996, "Defense Information System Network and Connected Systems"
- 3 DODD 5200.28, 21 March 1988, "Security Requirements for Automated Information Systems (AISs)"